



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/846,103      | 04/30/2001  | Dmitry O. Gryaznov   | 002.0160.01         | 5029             |

7590 03/15/2006  
ZILKA-KOTAB, PC  
P.O. BOX 721120  
SAN JOSE, CA 75172-1120

EXAMINER

COLIN, CARL G

ART UNIT PAPER NUMBER

2136

DATE MAILED: 03/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

|                              |                                      |  |  |
|------------------------------|--------------------------------------|--|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>09/846,103 | <b>Applicant(s)</b><br>GRYAZNOV ET AL. |  |
|                              | <b>Examiner</b><br>Carl Colin        | <b>Art Unit</b><br>2136                |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 13 December 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-5, 12, 13, 15, 17-21, 28, 29, 31, 33-35, 38-40, 43 and 44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5, 12, 13, 15, 17-21, 28, 29, 31, 33-35, 38-40, 43 and 44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Response to Arguments***

1. In response to communications filed on 12/13/2005, applicant has amended claims 1, 17, 33, 34, 38, 39, and 43-44; cancels claims 6-11, 22-27, 36-37, and 41-42. The following claims 1-5, 12-13, 15, 17-21, 28-29, 31, 33-35, 38-40, and 43-44 are presented for examination.

1.1 Applicant's arguments, pages 11-14, filed on 12/10/2004, with respect to the rejection of claims 1-44 have been fully considered, but they are not persuasive. Applicant argues that the prior art as combined does not teach "sets of indices and data files being organized into a hierarchy (emphasis added)". Examiner respectfully disagrees. Bates discloses a virus database with indices and data files being organized into a hierarchy, as disclosed by Bates it is well-known that a database may be an index and/or directory based database (see column 6, line 35 through column 8, line 15, with emphasis on column 8, lines 4-15 and column 11, lines 1-11) which implicitly has a hierarchical structure as data files are arranged in a well-organized manner. Chen et al discloses a data table including sets of instruction identifier stored in the virus information module (column 14, line 65 through column 15). Applicant states "only applicant teaches and claims a hierarchy of sets of indices and macro virus definition data organized based on a type of application to which the macro applies". As explained in Applicant's disclosure, page 8, "the database is hierarchically organized based on a type of application to which the macro applies." By way of example, the database can include a root directory, subdirectories of program applications such as (word processor, spreadsheet), and

generic subdirectories that may contain individual indices and macro virus definition data files (see figure 3). In other words, the disclosure merely discloses that macro virus data file (.dat), may be placed separately from other application. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a hierarchy of sets of indices and macro virus definition data organized based on a type of application to which the macro applies) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Besides, the specification does not teach a hierarchy of sets of indices and macro virus definition data. Applicant mentions that it appears that the Examiner has not taken into consideration organizing sets ...into hierarchy. Examiner would like to point out that it has been taken into consideration previously as interpreted by Examiner in light of the specification. It appears that Applicant's interpretation of the claim is not consistent with the specification and further clarification has been provided in this office action by Examiner. With respect to the amendment, applicant incorporates some of the elements of the cancelled claims such as claims 6-7 into the independent claims. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections. Applicant has not overcome the prior art as amended. Upon further consideration, the claims are still rejected in view of the same references.

*Claim Objections*

2. Claims 1, 17, and 34 are objected to because “the sets of indices and macro virus definition data files ...organized into a hierarchy ...to which the macro applies. It is not clear which macro is applied. Also, the phrase “the sets of indices and macro virus definition data files organized into a hierarchy” does not appear to be consistent with the specification referring to a database being organized into a hierarchy and not the sets of indices and macro virus definition data files; the sets of indices and macro virus definition data files are just part of the database. Appropriate correction is required.

*Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3.1 **Claims 1-5, 12-13, 15, 17-21, 28-29, 31, 33-35, 38-40, and 43-44** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,951,698 to Chen et al in view of US Patent 6,721,721 to **Bates et al** and in view of US Patent 5,448,668 to **Perelson et al**.

3.2 As per claims 1, 17, 33, 34, 39, and 44, **Chen et al.** substantially discloses a method and system for identifying a macro virus family using a macro virus definitions database, comprising: the macro virus definition data files and each macro virus definition data file defining macro virus attributes for known macro viruses that are comprised of at least one macro (columns 5-6). Column 5, lines 10-52 recite "a wide variety of application data files may be included in the memory such as word processing, spreadsheet, drawing programs, the memory may include Microsoft Word as Word processing, Excel as spreadsheet..." and further discloses (column 6, lines 10-67) "...examines targeted files to determine whether they are of a type that may include macro... whether the targeted file is a template file ... checking file extension such as .DOC. **Chen et al** clearly discloses a macro virus definition database being organized into a hierarchy based on the type of application to which the macro applies (as explained in columns 5-6). As interpreted by Examiner, Figure 9, shows also a virus information module (as part of the database) including data table with set of indices and macro virus definition data files organized also into a hierarchy as **Chen et al** discloses in (column 8, line 20 through column 9, line 15) indices and macro virus definition data files are associated with respect to file template format that meets the recitation of based on the type of application to which the macro applies. **Chen et al** discloses using file types for associating macro so that macros can be located (column 12). Further evidence of well-known database organized into hierarchy is shown by another reference of **Chen US Patent (5,960,170)**, which discloses data tables (figures 4a-4d) that provide example of how virus information are indexed based on file types, virus type, etc.. as previously explained in prior office action. **Chen et al.** discloses iteratively retrieving each macro virus definition

Art Unit: 2136

data file using the index for each macro virus family and providing the macro virus attributes defined in the retrieved macro virus definition data file, for example (see columns 12-14 and column 15). **Chen et al.** discloses wherein the macro virus definitions database storing string constants common to each macro virus family in the macro virus attributes for the macro virus definition data files, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15); and the macro virus checker comparing the suspect string to the string constants in the one or more macro virus definition data files for each macro virus family, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15). **Chen et al** discloses wherein a parameter specifying a threshold to matches of commonly shared string constants, for example (see column 15, lines 1-12). It is apparent to one with ordinary skill in the art that the virus information module comprising index and data files may be placed under any directory as a design choice according to the macro it as Chen suggests the module is separate from the other modules so the virus information may be easily updated and facilitate more efficient information transfer (see column 9, lines 15-30) being organized into hierarchy may be placed in any directory based on the macro it contains in Chen are diAssociating indexes based on the type of application is also common in the art. **Bates et al** discloses a database comprises set of indexes and macro virus status information with indexes associated with particular files (column 6, line 35 through column 7); files may also be organized according to type of application to make it easier to be identified (column 8, line 65 through column 9; and column 12, line 15 through column 13, line 35). **Bates et al** discloses that one of the advantages of organizing files according to file types and associating index with the data files is that it makes it easier to

Art Unit: 2136

different degrees of trustworthiness in the files based on viral infection and easier for searching, updating, and identifying information in the database. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of Chen et al to provide a database using index-based database referencing one or more of the macro virus definition data files and organizing the sets of the indices and the macro virus definition data files into a hierarchy according to macro virus families based on a type of application to which the macro applies as known in the art and as suggested by **Bates et al**. One skilled in the art would have been lead to make such a modification to benefit of the advantages mentioned above, for instance, because using index allows retrieval of any information associated with the index and also accelerates the search as suggested by **Bates et al** (column 2, lines 16-45 and column 6, line 35 through column 8, line 15).

**Chen et al** discloses parsing a suspect file into tokens comprising one of individual string constants and source code text and storing the tokens as suspect strings (columns 13-16). Chen et al discloses comparing a suspect string to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database, for example (see column 14, line 52 through column 15); and determining each macro virus family to which the suspect string belongs from the index for each macro virus definition data file at least partially containing the suspect string or file, for example (see column 13, line 20 through column 14 and column 14, line 52 through column 15). Chen et al does not explicitly disclose using a hierarchical parse tree, which is also well known. **Perelson et al** discloses parsing a suspect file into tokens comprising one of individual string constants and source code text and storing the tokens as suspect strings into a hierarchical parse tree (Column 2, line 50



Art Unit: 2136

through column 42 and column 7, line 45 through column 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of Chen et al to use a parse tree to store suspect strings because when there is more than one match it provides an efficient way to obtain results from different locations (column 7, line 45 through column 8) as taught by **Perelson et al.** One skilled in the art would have been lead to make such a modification to benefit from obtaining results from different locations in cases in which there may be more than one match as suggested by **Perelson et al** (column 7, line 45 through column 8).

**As per claims 2 and 18, Chen et al.** discloses the limitation of further comprising: the macro virus definition data files being indexed into the macro virus families categorized by a replication method employed, for example (see column 8).

**As per claims 3 and 19, Chen et al.** discloses the limitation of wherein the suspect string comprises part of a suspect file comprising a plurality of individual suspect strings, for example (see columns 14-15).

**As per claims 4 and 20, Chen et al.** discloses the limitation of further comprising: the macro virus checker identifying a replication method substantially common to a plurality of the individual suspect strings in the suspect file, for example (see column 14, lines 16 et seq.).

**As per claims 5 and 21, Chen et al.** discloses the limitation of further comprising: the macro virus checker identifying the macro virus family by which the common replication method is indexed, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

**As per claims 12, 13, 28, and 29, Chen et al.** substantially discloses the limitation of updating information when new virus is found which includes updating the index by writing new information to corresponding set of data that meets the recitation of further comprising: the macro virus checker resetting the index referencing one or more of the macro virus definition data files for at least one macro virus family and creating a new macro virus definition data file entry comprising an index referencing one or more macro virus definition files, for example (see column 9, lines 15 see also figure 9) and discloses the new macro virus definition data file entry defining the macro virus attributes by storing at least one of a. string constant and source code text, for example (see column 9 through column 10, line 27), Chen et al. is silent about resetting the index referencing one or more data files because it is obvious to one skilled in the art that to add new identifier the order may need resetting. Therefore, resetting the index referencing one or more of the macro virus definition data files for at least one macro virus family does not depart from the spirit and scope of the invention disclosed by **Chen et al.**

**As per claims 15 and 31, Chen et al.** discloses the limitation of further comprising: the macro virus checker cross referencing at least one of a string constant and source code text from

the parsed macro file attributes against: the macro virus attributes defined in the virus definition data files, for example (see columns 12-14).

**As per claims 35 and 40, Chen et al.** discloses the limitation of further comprising: each macro virus family defined according to a replication method substantially common to each of the macro virus definition data files associated with one such index, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

**As per claims 38, and 43, Chen et al.** discloses the limitation of further comprising: a parameter specifying a minimum length of commonly shared string constants, for example (see column 15, lines 1-12).

### *Conclusion*

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2136

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

March 8, 2006

CHRISTOPHER REVAK  
PRIMARY EXAMINER

cc 3/9/06